ref prev filed
Submitting
trans only

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-032567

(43)Date of publication of application : 03.02.1998

---

(51)Int.Cl. H04L 9/08
H04H 1/00
H04L 9/14
H04N 7/167

---

(21)Application number : 08-189636 (71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 18.07.1996 (72)Inventor : AKITA YASUTAKA

---

(54) CIPHERING EQUIPMENT, DE-CIPHERING EQUIPMENT AND DATA TRANSMISSION SYSTEM USING THEM

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a system with high security where ciphered media data are transmitted between a transmitter and a receiver and the data are not tapped by a 3rd party.

SOLUTION: In a transmitter, a continuous number extract means 20 and an identification number extract means 30 extract specific information of a media data consecutive number and an identification number from a header area of a packet 60. Then an initial value generating means 10 generates an initial value and a ciphering means 40 ciphers an information area of the transmission packet 60 based on the initial value. In a receiver, a consecutive number extract means 21 and an

identification number extract means 31 extract the media data consecutive number and the identification number from a header area of a reception packet 61. An initial value generating means 11 generates an initial value from them and a de-ciphering means 50 releases the ciphered information area in the received packet based on the initial value.

CLAIMS

[Claim(s)]

[Claim 1]A secrecy-ized device which secrecy-izes data stored in an information area of a packet which has a header area and an information area, and transmits a packet, comprising:

An extraction means to extract specific information of a header area of said packet.

An initial value generating means which generates an initial value based on said extracted specific information.

A secrecy-ized means to secrecy-ize data of an information area of said packet with an algorithm beforehand defined based on an initial value generated by said initial value generating means.

[Claim 2]It is a secrecy release device which outputs a packet which data of an information area of a packet which has a header area and an information area performed secrecy release processing of a secrecy-ized packet, and restored with a predetermined algorithm, An extraction means to extract specific information of a header area of said receive packet, and an initial value generating means which generates an initial value based on said extracted specific information, A secrecy release device provided with a secrecy release means which performs secrecy release of secrecy-ized data of an information area of said packet with a predetermined algorithm based on an initial value generated by said initial value

generating means, and outputs a restoration packet.

[Claim 3]A data communication system which secrecy-izes data stored in an information area of a packet which has a header area and an information area, and transmits and receives it, comprising:

1st extraction means by which a transmitting side device extracts specific information of a header area of a transmitting packet.

The 1st initial value generating means that generates an initial value for secrecy-izing data of an information area of a transmitting packet based on specific information extracted by said 1st extraction means.

The 2nd extraction means that is provided with a secrecy-ized means to secrecy-ize data of an information area of said packet based on an initial value generated by said 1st initial value generating means, and to transmit a packet, and extracts specific information of a header area of a receive packet in a receiving side device.

The 2nd initial value generating means that generates an initial value for canceling data in which an information area of a receive packet was secrecy-ized based on specific information extracted by said 2nd extraction means, A release means which cancels data in which an information area of a receive packet was secrecy-ized based on an initial value generated by said 2nd initial value generating means, and outputs a restoration packet.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]It is used when transmitting the packet which this invention packet-ized send data, such as media data, and performed secrecy-ization to the packet-ized data to a receiving set from a sending set, In order to avoid interception of the contents of the data by a third party, it is related with the secrecy-ized device which secrecy-izes data, the secrecy release device of which the secrecy-ized data is canceled, and the data transmission system using these.

[0002]

[Description of the Prior Art]When high-bandwidth-izing and the highly efficient compression encoding system of a transmission line have progressed in recent years, the data communications which transmit the media data of an image, a sound, etc. efficiently have spread. Introduction of the video conference system in a company, a paid broadcasting system, etc. is the example of representation. On the other hand, possibilities, such as interception of the confidential to the outside of the company information by a third party and unjust viewing and listening of the paid broadcasting

by a non subscription person, are also increasing as introduction of these systems spreads. In order to avoid such a situation, it is becoming general to carry out secrecy release of the media data which secrecy-ized media data by the sending set side with the specific secrecy-ized algorithm, and was secrecy-ized by the receiving set side, and to restore to the original media data.

[0003]In performing secrecy-ization of data in transmission of media data, especially transmission of the image as which real time nature is required, and the sound which accompanies this, By using a predetermined initial value, whenever divide into suitable length each media data which should be carried out [****]-izing, it blocks it, it secrecy-izes by a block unit and it starts secrecy-ized processing, It is common to make it that secrecy canceling becomes impossible [even if a bit error should occur within a secrecy-ized block on a transmission line, keep the error from affecting other secrecy-ized blocks, and] become only the specific secrecy-ized block which the bit error generated. Drawing 9 is a figure explaining operation in the CBC (CipherBlock Chaining) mode shown, for example in "the use mode of a 64-bit block cryptographic algorithm" (JIS X 5052, ISO 8372). An enciphering processing part is equivalent to the secrecy-ized means according to claim 1 among a figure. A decoding processing section is equivalent to the secrecy release means according to claim 2. In this mode, a cryptogram is fed back to the plaintext side in process of encryption processing. Encryption according E_K to the key K, decoding according D_K to the key K, and C_0 can be expressed like the following formula (1), when the plaintext i and C_i are made into the cryptogram i for an initial value and P_i.

[0004]

[Equation 1]

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = D_k(C_i) \oplus C_{i-1}$$

⊕…排他論理和

[0005]Initial value C_0 is an input value of the beginning for carrying out encryption processing of the blocked data. The cryptogram with same key which is different from the same plaintext when an initial value is changed but is generable. Therefore, encryption strength can be raised if an initial value is changed into a block unit.

[0006]Drawing 8 is the conventional secrecy-ized data transmission system shown in JP,63-167588,A. In a figure, the transmission data processing means 211 is a circuit which inputs the video signal 210 and performs secrecy-ization, and the output of the processing means 211 is led to the transmission line 213 via the data superposing means 212. The video signal 210 is supplied also to the number-of-times control means 214 of transmission. The number-of-times control means 214 of transmission counts the Vertical Synchronizing signal of the video signal 210, and is outputting the signals 214a, 214b, and 214c. Among these, the signal 214a is a signal which

**********s whenever a Vertical Synchronizing signal counts, and is inputted into the initial value conversion method 216. The output signals 214b and 214c of the number-of-times control means 214 of transmission are signals which give the timing which changes the initial value 215a.

For example, when changing an initial value for every n field, the maximum count value of the number-of-times control means 214 of transmission is set as n, and the signal 214b is outputted corresponding to counted value n at this time.

The new initial value 215a is generated in the timing of n counted value output 214b by this, and the superimposing data preparing means 217 chooses the output of the alignment pattern generating means 218 at the time of n count output, and chooses the initial value 215a as the other period. The initial value generating means 215 is maintaining the initial value 215a new from counted value n to n-1 of the following count cycle.

[0007]On the other hand, the initial value conversion method 216 has a function in which the above-mentioned new initial value 215a carries out the n field period latch output of the initial value 215a generated before to the timing generated from the initial value generating means 215.

The initial value before [this] carrying out a latch output receives predetermined logical conversion with each increment value of the signal 214a, and generates the random number signal 216a based on that translation data.

And the video signal inputted into the transmission data processing means 211 in the timing of this random number signal 216a to output is secrecy-ized. It is clear that it is a block unit of the data which the field unit of an image should carry out [****]-izing in this conventional example.

[0008]In this way, the video signal 225 secrecy-ized by making the above-mentioned translation data into an initial value is transmitted to the transmission line 213. The secrecy-ized video signal 219 from the transmission line 213 is supplied to the received-data processing means 220, the data extracting means 221, and the number-of-times counting means 222 of transmission. The received-data processing means 220 is a circuit which performs processing contrary to the transmission data processing means 211 by the side of a sending set, and carries out secrecy release of the secrecy-ized video signal 219. The data extracting means 221 is a circuit which all extracts [the whole field] the initial value on which it was superimposed at the prescribed period. The number-of-times counting means 222 of transmission counts the Vertical Synchronizing signal in the secrecy-ized video signal 219, and supplies the count output 222a to the initial value conversion method 223. In this case, a counter value is cleared by the signal 224a with which it shows the timing of that when an alignment pattern detection means 224 to carry out by which the number-of-times counting means 222 of transmission searches an alignment pattern detects an alignment pattern. Thereby, the initial value conversion method 223 will output the

same random number signal 223a as the sending set side, and the video signal 226 by which secrecy release was carried out correctly is outputted from the received-data processing means 220.

[0009]

[Problem(s) to be Solved by the Invention]The conventional secrecy-ized data transmission system is constituted as mentioned above, changes an initial value for every n field, and transmits the initial value which performed further predetermined logical conversion. However, although predetermined logical conversion was performed, the initial value appeared on the transmission line and there was a problem that this initial value is decoded by the third party, and secrecy release may be carried out, and it may be unjustly viewed and listened to the secrecy-ized data transmitted. While realizing secrecy-ized processing, without having been made in order that this invention might cancel the above problems, and transmitting an initial value between a sending set and a receiving set, It aims at obtaining the secrecy-ized data transmission system which divided into suitable length the data which should be carried out [****]-izing, and raised secrecy intensity in blocking, i.e., by using a predetermined initial value whenever it packet-izes and starts secrecy-ized processing of each packet.

[0010]

[Means for Solving the Problem]An extraction means for an invention of the 1st of this invention to be a secrecy-ized device which secrecy-izes data stored in an information area of a packet which has a header area and an information area, and transmits a packet, and to extract specific information of a header area of said packet, It has an initial value generating means which generates an initial value based on said extracted specific information, and a secrecy-ized means to secrecy-ize data of an information area of said packet with an algorithm beforehand defined based on an initial value generated by said initial value generating means.

[0011]An invention of the 2nd of this invention is a secrecy release device which outputs a packet which an information area of a packet which has a header area and an information area performed secrecy release processing of a secrecy-ized packet, and restored with a predetermined algorithm, An extraction means to extract specific information of a header area of said receive packet, and an initial value generating means which generates an initial value based on said extracted specific information, It has a secrecy release means which performs secrecy release of secrecy-ized data of an information area of said packet with a predetermined algorithm based on an initial value generated by said initial value generating means, and outputs a restoration packet.

[0012]An invention of the 3rd of this invention is a data communication system which secrecy-izes data stored in an information area of a packet which has a header area and an information area, and transmits and receives it, and a transmitting side device,

The 1st extraction means that extracts specific information of a header area of a transmitting packet, The 1st initial value generating means that generates an initial value for secrecy-izing data of an information area of a transmitting packet based on specific information extracted by said 1st extraction means, Have a secrecy-ized means to secrecy-ize data of an information area of said packet based on an initial value generated by said 1st initial value generating means, and to transmit a packet, and in a receiving side device. The 2nd extraction means that extracts specific information of a header area of a receive packet, The 2nd initial value generating means that generates an initial value for canceling data in which an information area of a receive packet was secrecy-ized based on specific information extracted by said 2nd extraction means, It has a release means which cancels data in which an information area of a receive packet was secrecy-ized based on an initial value generated by said 2nd initial value generating means, and outputs a restoration packet.

[0013]

[Embodiment of the Invention]

Below embodiment 1. describes the 1 embodiment of this invention about a figure. Drawing 1 is a figure showing the 1 embodiment of the secrecy-ized data transmission system concerning this invention. The figure and drawing 3 in which the composition of the packet transmitted with the secrecy-ized data transmission system which drawing 2 requires for this invention is shown, The figure showing the composition of the packet before secrecy-izing and after secrecy release, and a secrecy-ized packet, The figure showing the timing chart of secrecy-ized processing of a packet and secrecy release processing which drawing 4 requires for this invention, the figure showing the composition of the initial value generating means which drawing 5 requires for this invention, the figure showing the composition of the secrecy-ized means which drawing 6 requires for this invention, and drawing 7 are the figures showing the composition of the secrecy release means concerning this invention. The timing chart shown by drawing 4 is for explanation of this invention of operation, and does not specify strict timing.

[0014]As for 10 and 11, in drawing 1, a continuous number extract means, and 30 and 31 are identification number extracting means an initial value generating means, and 20 and 21. As for 40, a secrecy release means and 100 are transmission lines a secrecy-ized means and 50. A transmitting packet and 61 are secrecy-ized packets and 63 of 60 is the same as that of the transmitting packet 60 at a secrecy release packet. 70 and 71 are the identification numbers which identify the kind of data of media data etc., and are the numbers uniquely assigned according to the kind of data of the media data etc. which were stored in the information area of a packet. how to set predetermined in order whenever 80 and 81 are continuity numbers and it transmits a packet -- an order -- the price -- **** -- a number -- it is . Here, in this embodiment, make the sequence number and identification number of a header area

into specific information, and let a continuous number extract means and an identification number extracting means be extraction means to extract the specific information of a header area. In drawing 2, 64 is a header area of a packet and 65 is an information area of a packet. Media data is stored in the information area 65. An above-mentioned media data identification number and continuity number are stored in the header area 64. In drawing 3, the composition of the packet by which (a) stored the media data before secrecy-izing and after secrecy release in the information area, and (b) show the composition of the packet which stored the secrecy-ized media data in the information area.

[0015]In a sending set, the period until the transmitting packet 60 is outputted as the secrecy-ized packet 61 is explained using drawing 1, drawing 4, drawing 5, and drawing 6. The transmitting packet 60 is supplied to the identification number extracting means 30, the continuous number extract means 20, and the secrecy-ized means 40, and the composition is as being shown in drawing 2. The identification number extracting means 30 inputs the transmitting packet 60 which stored media data in the information area, In order to detect the header area of the packet concerned and to identify the media data concerned, the media data identification number 70 assigned uniquely is extracted from the header area, and it outputs to the initial value generating means 10. At this time, the identification number extracting means 30 has a function which carries out output maintenance until it will output to the initial value generating means 10 promptly and the information area 65 of the transmitting packet 60 will be inputted at least, if the media data identification number 70 is detected as shown in (a) of drawing 4.

[0016]The continuous number extract means 20 inputs the same packet 60 as the packet inputted into the identification number extracting means 30, extracts the continuity number 80 which detects the header area of the packet concerned and shows the continuity of the packet transmitted from the header area, and outputs it to the initial value generating means 10. At this time, the continuous number extract means 20 has a function which carries out output maintenance until it will output to the initial value generating means 10 promptly and the information area 65 of the transmitting packet 60 will be inputted at least, if the continuity number 80 is detected as shown in (a) of drawing 4. The initial value generating means 10 inputs the media data identification number 70 and the continuity number 80 of a packet which transmit from the identification number extracting means 30 and the continuous number extract means 20, respectively, The initial value 90 required in order to secrecy-ize the media data which carries out based on the combination of these media data identification numbers 70 and continuity numbers 80, and is stored in the information area of the packet concerned is generated, and it outputs to the secrecy-ized means 40. At this time, as shown in (a) of drawing 4, when both both the media data identification number 70 and the continuity number 80 are inputted, the initial value

generating means 10 generates the initial value 90 promptly, and outputs it to the secrecy-ized means 40, It has a function which carries out output maintenance until the information area 65 of the transmitting packet 60 is inputted at least.

[0017]The example of composition of the initial value generating means 10 is shown in drawing 5. They are held at the register 111 and the register 112, respectively until the media data identification number 70 and the continuity number 80 have the next input. In the operation part 113, the media data identification number 70 and the continuity number 80 which were held at the register 111 and the register 112 are inputted, it calculates by a predetermined method, and the specific address of the memory 114 with which two or more initial values (inside of a figure, C01-C0k) were stored is generated. At this time, the operation part 113 carries out the operation which uses addition, subtraction, multiplication, or division based on the media data identification number 70 and the continuity number 80 which are inputted. The memory 114 reads the initial value corresponding to the address given from the operation part 113 from the storing region, and outputs it as the initial value 90.

[0018]The secrecy-ized means 40 inputs the initial value 90 corresponding to the transmitting packet 60 from the initial value generating means 10, secrecy-izes the media data stored in the information area of the packet concerned, and outputs it as the secrecy-ized packet 61. At this time, the secrecy-ized means 40 loads the initial value 90, just before the media data of the information area 65 of the packet 60 concerned is inputted, as shown in (a) of drawing 4, and even the data of the last of the information area 65 continues and it carries out secrecy-ized processing as shown in drawing 9. Since the secrecy-ized means 40 does not perform secrecy-ization about a header area, the secrecy-ized packet 61 outputted as shown in (b) of drawing 3 serves as composition with the header area which is not secrecy-ized and the secrecy-ized information area.

[0019]The example of composition of the secrecy-ized means 40 is shown in drawing 6. The header separation part 401 separates the header area 64 and the information area 65 from the inputted transmitting packet 60, and outputs them to the header register 403 and the secrecy-ized treating part 402, respectively. The secrecy-ized treating part 402 carries out secrecy-ized processing using the initial value 90 given to the information area 65. The header register 403 holds the separated header area 64 temporarily. The header adjunct 404 adds the header area 64 temporarily held with the header register 403 to the information area 65 where secrecy-ized processing was carried out by the secrecy-ized treating part 402, and outputs it as the secrecy-ized packet 61. The secrecy-ized packet 61 by which the information area was secrecy-ized by the transmission line 100 as mentioned above is transmitted.

[0020]In a receiving set, the secrecy-ized packet 61 explains the period until it is outputted as the packet 63 by which secrecy release was carried out using drawing 1, drawing 4, drawing 5, and drawing 7. The secrecy-ized packet 61 to input is supplied to

the identification number extracting means 31, the continuous number extract means 21, and the secrecy release means 50 from the transmission line 100, and the composition is as being shown in drawing 2. In order to input the secrecy-ized packet 61, to detect the header area of the packet concerned and to identify the media data concerned, the identification number extracting means 31 extracts the media data identification number 71 assigned uniquely from the header area, and outputs it to the initial value generating means 11. At this time, the identification number extracting means 31 has a function which carries out output maintenance until it will output to the initial value generating means 11 promptly and the information area 65 of the secrecy-ized packet 61 will be inputted at least, if the media data identification number 71 is detected as shown in (b) of drawing 4.

[0021]The continuous number extract means 21 inputs the same packet 61 as the packet inputted into the identification number extracting means 31, detects the header area of the packet concerned, extracts the continuity number 81 which shows the continuity of a transmission **** packet from the header area, and outputs it to the initial value generating means 11. At this time, the continuous number extract means 21 has a function which carries out output maintenance until it will output to the initial value generating means 11 promptly and the information area 65 of the secrecy-ized packet 61 will be inputted at least, if the continuity number 81 is detected as shown in (b) of drawing 4. The initial value generating means 11 inputs the media data identification number 71 and the continuity number 81 of the secrecy-ized packet 61 which were received from the identification number extracting means 31 and the continuous number extract means 21, respectively, The initial value 91 required in order to carry out secrecy release of the media data which carries out based on the combination of these media data identification numbers 71 and continuity numbers 81, and is stored in the information area of the packet concerned is generated, and it outputs to the secrecy release means 50. At this time, as shown in (b) of drawing 4, when both both the media data identification number 71 and the continuity number 81 are inputted, the initial value generating means 11 generates the initial value 91 promptly, and outputs it to the secrecy release means 50, It has a function which carries out output maintenance until the information area 65 of the secrecy-ized packet 61 is inputted at least. Since the example of composition of the initial value generating means 11 is the same as that of drawing 5 in which the example of composition of the initial value generating means 10 is shown and the operation is also the same, explanation is omitted.

[0022]The initial value 91 corresponding to the secrecy-ized packet 61 which received is inputted from the initial value generating means 11, and secrecy release of the media data stored in the information area of the packet concerned is carried out, it restores to the original packet 63, and the secrecy release means 50 outputs this. At this time, the secrecy release means 50 loads the initial value 91, just before the

media data of the information area 65 of the packet 61 concerned is inputted, as shown in (b) of drawing 4, and even the data of the last of the information area 65 continues and it carries out secrecy processing as shown in drawing 9. The example of composition of the secrecy release means 50 is shown in drawing 7. The header separation part 501 separates the header area 64 and the secrecy-ized information area 65 from the inputted secrecy-ized packet 61, and outputs it to the header register 503 and the secrecy release processing section 502, respectively. The secrecy release processing section 502 carries out secrecy release processing using the initial value 91 given to the secrecy-ized information area 65. The header register 503 holds the separated header area 64 temporarily. The header adjunct 504 adds the header area 64 temporarily held with the header register 503 to the information area 65 where secrecy release processing was carried out by the secrecy release processing section 502, and outputs it as the secrecy release packet 63.

[0023]Drawing 2 in which the composition of a packet is shown is explained further. The header area 64 is a field where the control information on the packet concerned is stored, and the media data identification number and the continuity number are stored at least in control information. The information area 65 is a field where the media data divided into suitable data length is stored. The number of the media data stored in the information area in one packet is one. A media data identification number is given by the sending set side, it is the identification number uniquely assigned according to the kind of media data stored in the information area 65, and a receiving set judges the kind of media data which detected this media data identification number and was stored in the packet concerned. Whenever a continuity number is given by the sending set side and it transmits a packet, it is the number which was able to be set in order by how to set predetermined in order, and a receiving set judges the existence etc. of a loss of the packet which received by supervising the continuity of this continuity number. Therefore, a media data identification number and a continuity number are not the information for secrecy-ized processing for the purpose of the original above-mentioned processing, and it is the feature of this invention to use a media data identification number and a continuity number for secrecy-ized processing and secrecy release processing.

[0024](a) of drawing 3 shows the composition of the transmitting packet 60 and the packet 63 (namely, the original transmitting packet 60) by which secrecy release was carried out, and (b) shows the composition of the secrecy-ized packet 61. If the media data of the information area of the transmitting packet 60 of the composition of (a) is secrecy-ized by the secrecy-ized means 40, it will become the secrecy-ized packet 61 of the composition of (b). At this time, the object of secrecy-ized processing is only an information area of a packet, and a header area is not secrecy-ized. On the other hand, secrecy release is carried out by the secrecy release means 50, and the media data of the information area of the secrecy-ized packet 61 of the composition

of (b) serves as the packet 63 of the composition of (a), and is restored to the original transmitting packet 60.

[0025]

[Effect of the Invention]With the secrecy-ized device by this invention, a secrecy release device, and the data transmission system using these, as mentioned above. Since an initial value is not transmitted via a transmission line between a sending set and a receiving set, it is effective in secrecy release of the secrecy-ized data which an initial value is not monitored by a third party, therefore is transmitted being done by the third party, and being able to prevent that unjust viewing and listening is carried out. Since it had composition using a predetermined initial value whenever it started secrecy-ized processing of each packet, there is an effect which can raise secrecy intensity further.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a figure showing the composition of the secrecy-ized data transmission system concerning this invention.

[Drawing 2]It is a figure showing the composition of the packet transmitted with the secrecy-ized data transmission system concerning this invention.

[Drawing 3]It is a figure showing the composition of the packet before secrecy[in the secrecy-ized data transmission system concerning this invention]-izing, and after secrecy release, and a secrecy-ized packet.

[Drawing 4]It is a figure showing the timing chart of secrecy-ized processing of a packet, and secrecy release processing in the secrecy-ized data transmission system concerning this invention.

[Drawing 5]It is a figure for explaining the composition of the initial value generating means in the secrecy-ized data transmission system concerning this invention.

[Drawing 6]It is a figure for explaining the composition of the secrecy-ized means in the secrecy-ized data transmission system concerning this invention.

[Drawing 7]It is a figure for explaining the composition of the secrecy release means in the secrecy-ized data transmission system concerning this invention.

[Drawing 8]It is a figure showing the composition of the conventional secrecy-ized data transmission system.

[Drawing 9]It is a figure explaining operation in the CBC (CipherBlock Chaining) mode shown in "the use mode of a 64-bit block cryptographic algorithm" (JIS X 5052, ISO 8372).

[Description of Notations]

10 and 11 An initial value generating means, 20, and 21 Continuous number extract means, 30 and 31 An identification number extracting means and 40 A secrecy-ized means and 50 Secrecy release means, 60 transmitting packet and 61 [An information area, 70, and 71 / A continuity number, 90, and 91 / An initial value and 100 / Transmission line.] A media data identification number, and 80 and 81 A secrecy-ized packet and 63 A secrecy release packet, 64 header areas, and 65